CPNI
Centre for the Protection of National Infrastructure

Biometrics – Selecting What is Right for You

PUBLISH DATE: June 2020

CLASSIFICATION: Official

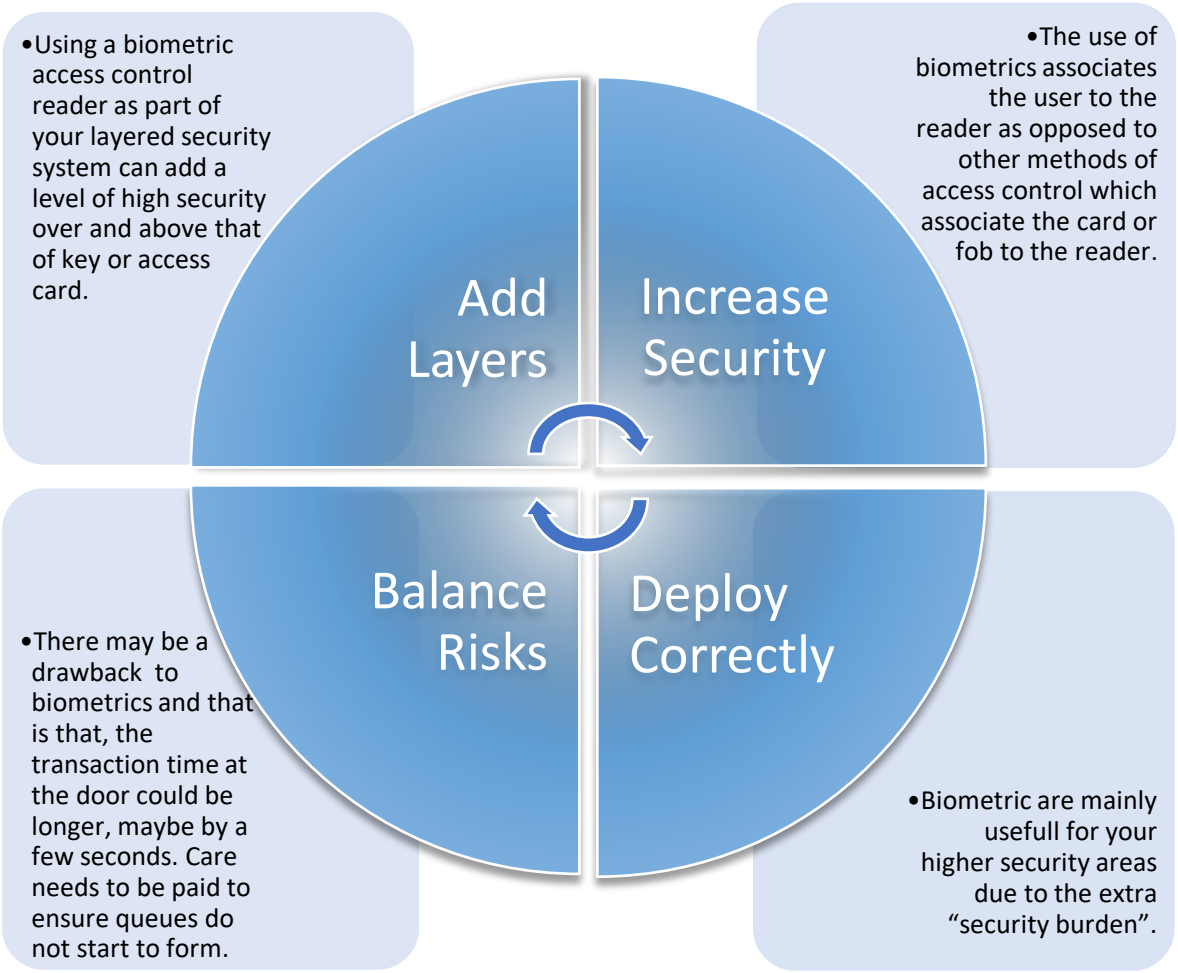
Biometrics - A Guide to Selecting What is Right for You

Version 2.0

Introduction

This short guide will set out some of the basic principals and things to consider when trying to decide whether or not a biometric access control system will be right for you. It should be used to inform thinking in the early stages of the Operational Requirement (OR) process.

It will not go into enough detail to fully inform a decision. The CPNI Biometrics For Automatic Access Control Systems (BAACS) Guidance will provide more information on BAACS generally. Specific modality information must be sought as part of the OR process and Equipment Specification stage.



Are Biometrics for Me?

Biometric technologies provide an aid to controlling access to a site or space. They should not be used on their own but in conjunction with another access control measure. It should be remembered that they may not be suitable for all applications. Listed below are some key factors to consider when making the initial decision whether to deploy biometric technologies in an access control environment.

- Biometric technologies can automatically recognise people already known to the system.
- How will you handle exception? These are vulnerable events
- Biometrics should not be used as 'stand-alone' systems: rather as part of an integrated access control system. An example might be a fingerprint used with a smartcard.
- Personal information used for enrolment must be verified at time of enrolment.
- The enrolment process can be complex and time consuming.
- Biometrics can operate, if required, without any further personal information being stored.
- It is possible to ensure that duplicate enrolments do not happen and to build in anti-tamper
- Biometrics are not infallible, cases of 'false positives' and 'false rejections' are possible.
- Biometrics may increase or decrease the time taken to access a site. This should be considered when selecting the technology. Some methods may be more suitable than others depending on situation.
- A program of 'enrolment' must be carried out before the system can be deployed.

Types of Biometric System

There are a number of commercially available biometric technologies based on a number of human characteristics.

Fingerprints

This is probably the best known technique. In modern access control applications, users place their finger onto the glass plate of a fingerprint scanner. A light shining from below reflects only where there is a fingerprint 'valley', not a ridge. This reflected image is recorded and stored. Normally two fingers would be scanned per subject. This allows for one fingerprint being damaged.

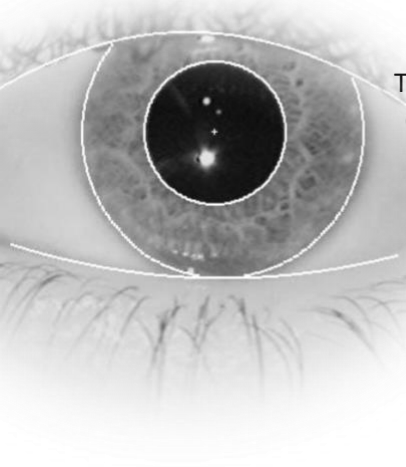
Face Recognition

This system uses a digital image of the subject for comparison. Consistency of pose, lighting and facial expression is required. The photograph must also be recent. These exacting requirements make this system difficult to manage in an access control application.

Hand Geometry

Hand shape has been used as a biometric technology for many years. It requires the hand to be placed on a reflective surface. Illumination from above reflects from the exposed part creating a silhouette of the hand which is captured by the camera. It is the shape of the hand only that is recorded, not the palm print or the fingerprint.

Iris Pattern

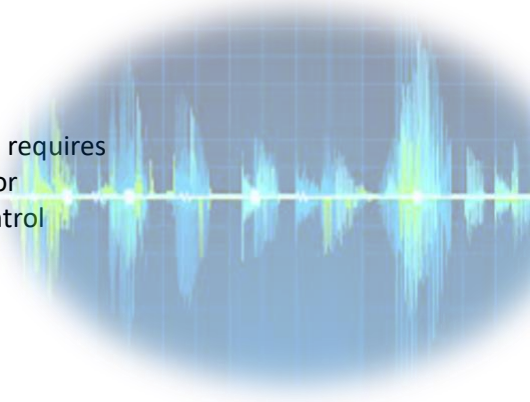


The iris has long been recognised as distinctive and individual. Iris recognition devices take a greyscale photograph of the iris pattern using an invisible and harmless infrared light for illumination. By processing the image, a binary code is produced. It is this code which is used for comparison. Although the image can be obscured by cosmetic contact lenses, standard lenses cause no problems. Iris recognition systems are accepted as one of the better biometrics techniques.

Finger/Palm Vein

This is a newer technique, though it well established, and involves the imaging of veins in the hand or finger. This system exploits the fact that veins absorb more near-infrared light than other types of tissue beneath the skin. The hand or finger is illuminated with low intensity infrared light which can be imaged with a standard CCD sensor. The light absorbing veins return a dark pattern against the more translucent skin and other tissue.

Voice Pattern



This technique uses the voice patterns of a subject for identification. This requires the subject to speak a known phrase. It is this exact phrase that is used for comparison. As yet there are no standards for voice biometric access control systems.

Some Important Questions

Before a biometric system is implemented there are a number of questions that need answering. These things will all be brought out in your OR. However it is well worth considering these now as biometrics can be really useful or really bad depending on what your requirement is. Looking at the considerations early might save a lot of time and money later.

- Will biometrics help? Why are tokens and readers not suitable?
- Is there a business case? Will there be extra cost? Cost savings?
- Are there any current legal or legislative issues to be considered?
- Will privacy be an issue? What data is being stored and who will have access to it?
- Will PINs and/or tokens be used as well? (2 Factor Authentication)
- How user friendly will the system be? Will training be required for a user?
- What are the risks of false positives and false rejections? (Threshold of approx. 2%)
- Will CCTV oversight be required?
- What will the environment be like? Outdoors, light levels, PPE, office, noisy, etc.
- What about people who can't use Biometric systems?